JOURNAL OF ALGEBRA **198,** 1–18 (1997)
ARTICLE NO. JA977181

Tori and Idempotents in Reduced Enveloping Algebras of a Solvable Lie p-Algebra

John R. Schue

Department of Mathematics and Computer Science, Macalester College

Communicated by Georgia Benkart

Received July 3, 1995

1. INTRODUCTION

1.1. Throughout the discussion L will denote a finite-dimensional Lie p-algebra over an algebraically closed field F of characteristic $p > 2$, and usually assumed to be solvable. In [11], we were able to obtain a decomposition of the division algebra $D(L)$ generated by L, expressing it as a kind of tensor product of two subfields: one separable, the other purely inseparable. Since the universal enveloping algebra $U(L)$ is embedded in $D(L)$, this decomposition gives some information on $U(L)$, but it is difficult to deal with because of the infinite dimensionality over F.

Here we will be primarily concerned with the structure of the reduced enveloping algebras associated with L and will be able to obtain more satisfactory results. A step in this direction can be found in [9] where the emphasis is on determining primitive idempotents for the restricted enveloping algebra. Our results here will be more complete and are applicable to any of the reduced enveloping algebras. From the structure theorems in Section 4 results are obtained regarding the nature of the radical, the simple components for a Wedderburn–Malcev decomposition, and the construction of a maximal torus. All of the results are constructive and make essential use of the solvability of L. In Section 5 we give a new construction for the irreducible representations. There is also a discussion indicating a method for obtaining information about the central idempotents and block structure for the reduced algebras, which would extend to a general solvable L results obtained by Farnsteiner [3] for L strongly solvable and Feldvoss [2] for L supersolvable.

0021-8693/97 $25.00

For notation, $P = \{0, 1, \ldots, p-1\}$ is the field of integers modulo p and P^m is the set of m-dimensional vectors $\alpha = (\alpha_1, \ldots, \alpha_m)$, $\alpha_i \in P$, with θ used to denote the zero vector in P^m. $U(L)$ is the universal enveloping algebra for L over F. For an ordered sequence $u_1, \ldots, u_m$ of elements in $U(L)$ and $\alpha \in P^m$ we set $u^\alpha = u_1^{\alpha_1} \cdots u_m^{\alpha_m}$. We regard L as embedded in $U(L)$.

The p-mapping on L will be denoted by $x \to x^{[p]}$. Suppose $x_1, \ldots, x_n$ is a basis for L and $z_i = x_i^p - x_i^{[p]} \in U(L)$. As noted in [5], p. 190, each z_i is in the center of $U(L)$ and $1, z_1, \ldots, z_n$ generate the polynomial algebra $F[z_1, \ldots, z_n]$, here denoted by $F[z]$. Then U has $\{x^\alpha\colon\ \alpha \in P^n\}$ as a basis over the ring $F[z]$.

If K is a p-subalgebra of F, for simplicity of notation, we will let $U(K)$ denote the respective subalgebras of U obtained by using the usual enveloping algebra for K with the base ring enlarged to $F[z]$. Thus, if $x_1, \ldots, x_m$ is a basis for K, Then $\{x^\alpha\colon\ \alpha \in P^m\}$ is a basis for $U(K)$ over $F[z]$. If K is an ideal of L, then $[L, U(K)] \subset U(K)$.

2. REDUCED ENVELOPING ALGEBRAS

2.1. The development in this section will not make use of the solvability of L and is applicable to any finite-dimensional Lie p-algebra over F. As in [2]–[4], for a linear map $\chi\colon L \to F$ we let $u(L, \chi)$ be the F-algebra obtained by taking $U(L)$ modulo the ideal $I(\chi)$ generated by $\{x^p - x^{[p]} - \chi(x)^p 1\colon\ x \in L\}$. We embed L in $u(L, \chi)$ by the map $x \to x + I(\chi)$. Then, for a basis $\{x_i\}$ of L, $\{x^\alpha\}$ is an F-basis for $u(L, \chi)$. A representation R of L, hence of $U(L)$, will be called a χ-representation if $R(x^p) = R(x^{[p]}) + \chi(x)^p 1$. In this case it will follow from Section 1 (and also from the development in [13, 5.1]), that $R(u) = \mu(u)1$ for all $u \in P[z]$, where μ is the unique homomorphism of $P[z]$ onto F such that $\mu(x^p - x^{[p]}) = \chi(x)^p$ for x in L. From this then it follows easily that $I(\chi) = \{\sum f_\alpha x^\alpha\colon\ \mu(f_\alpha) = 0\}$, $R(I(\chi)) = 0$, and R induces a representation of $u(L, \chi)$. Since every irreducible representation is a χ-representation for some χ, we obtain a partition of the set of all irreducible representations, with R, R' in the same class if and only if $\chi = \chi'$.

We will frequently regard $u(L, \chi)$ as a Lie algebra with $[u, v] = uv - vu = \delta(u)v$. It will be a p-algebra if we set $u^{[p]} = u^p$. We let $u \to u^*$ denote the unique anti-automorphism of $u(L)$ such that $x^* = -x$ for $x \in L$. The representation $x \to \delta(x)$ can be extended to a representation ∇ of $u(L)$ acting on $u(L)$ and it follows from [7, (1), p. 258] that $ux^\alpha = \sum C(\alpha, \beta) x^{\alpha-\beta} \nabla(x^\beta *)(u)$ for $x_1, \ldots, x_m \in L$, $u \in u(L)$, where for $\alpha \in P^m$, the sum is taken over all β with $\beta_i \le \alpha_i$, and $C(\alpha, \beta) = \prod C(\alpha_i, \beta_i)$, where $C(\alpha_i, \beta_i)$ is the usual binomial coefficient.

Since we are embedding L in $u(L)$ this gives rise to different interpretations for $x^{[p]}$ for x in L, but the interpretation should be clear from the context. Now any u in $u(L)$ can be expressed uniquely as $u = s + z$, where s is semisimple and u is nilpotent. From [6] it follows that s and z are p-polynomials in u and s is a linear combination of s_i, where $s_i^p = s_i$ and each s_i is a p-polynomial in s.

3. TORI IN ASSOCIATIVE ALGEBRAS

3.1. We continue to work in $u(L, \chi)$, though most results of this section are valid in any associative algebra with identity over F. A commutative semisimple associative subalgebra S containing 1 will be called a torus. If S is a torus and $s \in S$ with $s^p = s$ we let $e_i = e_i(s) = 1 - (s - i1)^{p-1} \in S$, $0 \le i \le p - 1$. Then it is easy to verify that $e_i e_j = \delta_{i,j} e_i$, $s = \sum i e_i$, and $1 = \sum e_i$. Since S is spanned by such s it follows that S has a basis $\{e_\rho\}$ of idempotents and these are necessarily orthogonal and minimal in S. Hence for each ρ, there is a unique homomorphism, also denoted by ρ, with $se_\rho = \rho(s)e_\rho$ and $\rho(1) = 1$. Conversely, given a homomorphism σ with $\sigma(1) = 1$ there will exist a unique e_ρ with $\sigma(e_\rho) = 1$ and hence $\sigma = \rho$ so that the index set $\{\rho\}$ can be identified with the set of all homomorphisms of S onto F.

3.2. EXAMPLE. Suppose T is a (Lie) torus in L. Then there exists a basis $\{t_i\colon i = 1, \dots, m\}$ for T with $t_i^{[p]} = t_i$. For each i if $\xi_i \in F$ is chosen such that $\xi_i^p - \xi_i = \chi(t_i)^p$, then for $s_i = t_i - \xi_i 1$ we have $s_i^p = s_i$. Then $u(T, \chi)$ is a torus in $u(L, \chi)$ with $\{s^\alpha\colon \alpha \in P^m\}$ as a basis. If, for $\rho \in P^m$, we set $e_\rho = \prod_i (1 - (s_i - \rho(i))^{p-1})$ then, as in [8, p. 192], $\{e_\rho\}$ will be a basis of orthogonal idempotents for $u(T)$.

3.3. More generally, a torus S of $u(L, \chi)$ will be called a p-torus if there exist $s_1, \dots, s_m \in S$ such that $s_i^p = s_i$ and $\{s^\rho\colon \rho \in P^m\}$ is a basis for S. Then, as for $u(T, \chi)$, we can use the s_i to construct a basis of idempotents for S.

For a p-torus S let $S_0 = \sum F s_i$. For a linear functional λ on S_0 let $R_\lambda(S) = \{u \in u(L)\colon [s, u] = \lambda(s)u \text{ for } s \in S_0\}$. We say λ is a root for S if $R_\lambda(S) \ne 0$. For any u, ρ, σ we have $[s, e_\rho u e_\sigma] = (\rho(s) - \sigma(s))e_\rho u e_\sigma$. Since $u = \sum_{\rho,\sigma} e_\rho u e_\sigma$ this implies $u(L, \chi)$ is the sum, necessarily direct, of the root spaces $R_\lambda(S)$ and the roots are the restrictions of $\{\rho - \sigma\}$ to S_0. If $S = u(T, \chi)$, where T is a torus in L and $y_1, \dots, y_n$ is a basis for L consisting of root vectors for T with $[t, y_i] = \lambda_i y_i$, then y^α is a root vector for S in the root space $R_{\sum \alpha_i \lambda_i}$.

We use $R(L, \chi)$ to denote the Jacobson radical of $u(L, \chi)$, i.e., the set of all elements of $u(L, \chi)$ annihilated by all irreducible χ-representations. Thus $R(L, \chi) \cap L = N(L, \chi)$, where $N(L, \chi)$ is the χ-nil radical of L, i.e., all x annihilated by all irreducible χ-representations of L. From now on it will be convenient, unless specified otherwise, to adopt the notation, for $u, v \in u(L, \chi)$, $u = v$ to mean congruence modulo $R(L, \chi)$.

3.4. PROPOSITION. *Let* $Z(L, \chi) = \{u: [u, u(L, \chi)] \equiv 0\}$. *Then we have*:

(1) $Z(L, \chi)$ *is an associative subalgebra of* $u(L, \chi)$ *containing the identity and* $R(L, \chi)$.

(2) $Z(L, \chi)$ *is a strongly solvable Lie p-ideal of* $u(L, \chi)$.

(3) $Z(L, \chi)/R(L, \chi)$ *is the center of* $u(L, \chi)/R(L, \chi)$.

(4) $Z(L, \chi) = SZ(L) \oplus R(L, \chi)$, *where* $SZ(L)$ *is a maximal torus in* $Z(L, \chi)$.

Proof. (1)–(3) follow directly from the definition. (4) follows easily from the Wedderburn–Malcev theorem (see [1, p. 491]) but also follows from the Lie theory for p-algebras because of (2).

3.5. We have $[SZ(L), u(L)] \equiv 0$ and will say that $SZ(L)$ is a radical torus. The canonical homomorphism of $u(L, \chi)$ onto the quotient modulo $R(L, \chi)$ will be an isomorphism of $SZ(L)$ onto the center. Now $SZ(L)$ has a basis $\{e_\rho\}$ of orthogonal idempotents and each coset $e_\rho + R(L, \chi)$ is then a primitive central idempotent in $U(L, \chi)/R(L, \chi)$. Each e_ρ will be called a primitive radical idempotent.

Now $u(L, \chi)/R(L, \chi)$ is a semisimple associative algebra over F and hence is a direct sum of orthogonal simple matrix algebras. The construction above then gives $\{e_\rho + R(L, \chi)\}$ as a complete set of orthogonal central idempotents in the quotient. Thus $R(L, \chi) = \sum R(L, \chi)e_\rho$, $u(L, \chi)e_\rho/R(L, \chi)e_\rho$ is a simple matrix algebra, and $u(L, \chi)/R(L, \chi)$ is the direct sum of the ideals $u(L, \chi)e_\rho/R(L, \chi)e_\rho$. For each ρ there is an irreducible representation R_ρ of $u(L, \chi)$ with $R_\rho(e_\rho) = 1$ and R_ρ is unique up to equivalence. Any irreducible R is equivalent to some R_ρ and the kernel for R_ρ is $R(L)e_\rho + \sum u(L)e_\sigma$, $\sigma \neq \rho$. It is useful to note that $u(L, \chi)e_\rho = e_\rho u(L, \chi)e_\rho + (1 - e_\rho)u(L, \chi)e_\rho$ and the latter term lies in $R(L, \chi)$ since it is equal to $\{u: [e, u] = -u\}$. Thus $u(L, \chi)e_\rho/R(L, \chi)e_\rho$ is isomorphic to $e_\rho u(L, \chi)e_\rho/e_\rho R(L, \chi)e_\rho$.

In the next section we will show that for L solvable, a maximal torus for L will give rise to a maximal radical p-torus $SZ(L)$ with $[T, SZ(L)] = 0$ and this in turn will allow construction of a maximal torus for $u(L, \chi)$ containing $SZ(L)$ and $u(T, \chi)$ and which will also be a p-torus.

3.6. PROPOSITION. *For $SZ(L)$ as above, let $u(\rho, \sigma) = e_\rho u(L) e_\sigma$. Then we have the following*:

(1) $u(L, \chi) = \oplus \sum u(\rho, \sigma)$.

(2) *For* $\rho \neq \sigma$, $u(\rho, \sigma) \subset \{u: [e_\rho, u] = u\} = \{u: [u, e_\sigma] = -u\} \subset R(L, \chi)$.

(3) $\oplus \sum u(\rho, \rho)$ *is equal to* $\{u: [SZ(L), u] = 0\}$.

(4) $u(\rho, \sigma) u(\tau, \upsilon) = 0$ *for* $\sigma \neq \tau$.

Proof. (1)–(4) all follow directly from the definitions.

3.7. We will concentrate here primarily on the structure of the diagonal terms $u(\rho, \rho)$, and the structure theorems deal with these. The off-diagonal terms all lie in $R(L, \chi)$, and will be important in any detailed description of the block structure for $u(L, \chi)$, but we will not consider them here in detail.

3.8. EXAMPLE. To illustrate the role of χ we consider the algebra L_2 with basis $\{t, a\}$ and $t^{[p]} = t$, $a^{[p]} = 0$. For $\chi = 0$ we have $N(L, \chi) = Fa$, $R([L, L]) = 0$ for any χ-irreducible representation, and L is strongly solvable.

If, however, we use χ with $\chi(t) = 0$, $\chi(a) = 1$, then, in $u(L, \chi)$, $a^p = 1$ and $N(L, \chi) = 0$. We can obtain an irreducible R acting on V, where V has basis $\{v_0, \ldots, v_{p-1}\}$ and $R(t)v_i = iv_i$, $R(a)v_i = -iv_{i+1}$, and subscripts are taken modulo p. Thus $R(u(L, \chi))$ must be a simple algebra of dimension p^2 so that R is faithful and $u(L, \chi)$ is simple.

This admits the following generalization. Let L_{2r} have basis $\{t_i, a_i: i = 1, \ldots, r\}$. L_{2r} becomes a p-algebra if we use the relations $[t_i, a_i] = a_i$, $t_i^{[p]} = t_i$, $a_i^{[p]} = 0$, (L_{2r} is the direct sum of r copies of L_2), and define χ by $\chi(t_i) = 0$, $\chi(a_i) = 1$. Thus $t_i^p = t_i$, $a_i^p = 1$, $S = \sum t^\alpha$ is a p-torus, and $A = \sum a^\alpha$ is a commutative subalgebra with $[t_i, A] \subset A$. We let $d_i = a_i^{p-1} t_i$ and $b_i = a_i - e$. Then $[d_i, b_j] = \delta_{i,j} 1$ and $[d_i, d_j] = 0 = d_i^p = b_i^p$. Thus $[b_i, d^\alpha] = -\alpha_i d^{\alpha - \varepsilon_i}$, where ε_i is the usual unit vector. We also have $\{d^\alpha b^\beta\}$ as a basis for $u(L, \chi)$.

Suppose R is an irreducible representation of L_{2r} on V and v_0 is a nonzero vector in V with $R(b_i)v_0 = 0$ for all i. Thus V is spanned by $\{R(d^\alpha)v_0\}$. By the same argument as used in [7], for Theorem 1 it follows that the spanning set is also linearly independent and hence $\dim(V) = p^r$. Thus, as above, R must be faithful and $u(L_{2r})$ is simple. A variation on this is to take s with $1 \leq s < r$ and set $\chi(a_i) = 1$ for $i \leq s$ and $\chi(a_i) = 0$ for $i > s$. Then $N(L_{2r}, \chi) = \sum Fa_i$, $i > s$, and $u(L_{2r}, \chi) = S + I$, where I is the nil ideal generated by $N(L_{2r}, \chi)$ and $S = \sum Ft^\alpha a^\beta$, and the a_i are chosen with $i \leq s$. Then S will be semisimple with $\sum Ft^\beta$ as a maximal radical torus, where the t_i are chosen with $i > s$ and $I = R(L, \chi)$.

It is possible to modify this example to obtain one with $\chi = 0$ by adding an additional central element t_0 to the basis and setting $t_0^{[p]} = t_0$ and $a_i^{[p]} = t_0$. In this case the idempotent decomposition of t will give $u(L)$ as a sum of p simple ideals and hence is semisimple. An alternative presentation is to define L'_{2r+1} with basis $\{t_0, d_i, b_i: i = 1, \ldots, r\}$, $\chi = 0$, $t_0^{[p]} = t_0$, $d_i^{[p]} = b_i^{[p]} = 0$, and $[d_i, b_j] = \delta_{i,j} t_0$. This gives the Heisenberg algebra of [2, Example 2].

4. THE STRUCTURE THEOREMS

4.1. From now on we will assume L is solvable and will devote most of this section to the development of the structure theorems, as stated in 4.3 and 4.17. It will be convenient to regard χ as fixed and omit it in notation. Thus $u(L) = u(L, \chi)$, etc. To illustrate ideas and some of the results on blocks as obtained in [3], we begin with the case when L is strongly solvable, i.e., $[L, L] \subset N(L, \chi)$. We continue to use $u \equiv v$ to mean congruence modulo $R(L)$.

4.2. STRUCTURE THEOREM FOR L STRONGLY SOLVABLE. *Suppose L is strongly solvable, T is a maximal torus for L, and $T_C = \{t \in T: [t, L] = 0\}$. Let $\{t_i: 1 \le i \le h\}$ be a basis for T with $t_i^{[p]} = t_i$ such that $\{t_i: 1 \le i \le c\}$ is a basis for T_C, and choose $\{s_i\}$ as in* 3.2. *For a homomorphism ρ of $u(T)$ let e_ρ be defined as in* 3.2 *and define f_ρ similarly but using T_C rather than T. (If $h = 0$, e_ρ is defined as* 1 *and similarly for f_ρ if $c = 0$.) Then*:

(1) *$u(L) = u(T) \oplus R(L)$ and $R(L) = u(L)N(L)$.*

(2) *The radical p-torus $u(T)$ is a maximal torus for $u(L)$.*

(3) *$\{f_\rho\}$ is a complete orthogonal set of primitive central idempotents for $u(L)$ and $f_\rho = \sum e_\sigma$ with the sum taken over all σ such $\sigma(s) = \rho(s)$ for all s in $u(T_C)$.*

(4) *$e_\rho u(L) e_\rho = F e_\rho + e_\rho R(L) e_\rho$.*

(5) *The blocks of $u(L)$ are the ideals $f_\rho u(L)$ and $f_\rho u(L) = \sum e_\sigma u(L) e_\tau$, taken over all σ, τ with $\sigma = \tau$ on $u(T_C)$.*

(6) *Let I_ρ be the ideal of $u(L)$ generated by $\{t_i - \rho(t_i)1: 1 \le i \le c\}$. Then the block $f_\rho u(L)$ is isomorphic to $u(L)/I_\rho$.*

Proof. L strongly solvable implies $L = T \oplus N(L)$ and we choose $\{x_j\} \subset N(L)$ as a basis for L supplementary to T. Then the Poincaré–Birkoff–Witt theorem gives $u(L) = u(T) \oplus I$, where I is the ideal $N(L)u(L)$. Thus $I \subset R(L)$ and $u(T)$ semisimple implies $I = R(L)$.

Necessarily $u(T)$ is a radical torus in $u(L)$. To show it is maximal, suppose $s \in u(L)$ with $s^p = s$ and $[s, u(T)] = 0$. Now $s = s_T + z$ for some

$s_T \in u(T)$, $z \in R(L)$, so that $s = s^{p^k} = s_T^{p^k}$ for k sufficiently large and $s \in u(T)$. Thus $u(T)$ is a maximal torus in $u(L)$.

The first assertion of (3) follows directly from the definitions. For the second assertion the definitions give $f_\rho e_\sigma = e_\sigma$ is and only if $\rho = \sigma$ on $u(T_C)$ while $f_\rho e_\sigma = 0$ if $\rho \neq \sigma$ on $u(T_C)$. Since $1 = \Sigma e_\sigma$ the second assertion follows.

For (4), $e_\rho u(T) = Fe_\rho$ so (1) gives $e_\rho u(L) e_\rho = Fe_\rho + e_\rho R(L) e_\rho$.

For (5), we have $\{f_\rho\}$ as a complete set of orthogonal central idempotents and hence the blocks are the ideals $f_\rho u(L)$. The sum is a consequence of the decomposition for f_ρ and $f_\rho u(L) f_\rho = f_\rho u(L)$.

(6) The mapping $u \to e_\rho u$ is an algebra homomorphism and it suffices to prove the kernel K_ρ is I_ρ. Since $e_\rho \in u(T_C)$ it follows from the Poincaré–Birkhoff–Witt theorem that K_ρ is the ideal $u(L)S_\rho$, where $S_\rho = \{u \in u(T_0)\colon e_\rho u = 0\}$ and is the ideal generated by $\{t_i - \rho(t_i)1\}$.

4.3. For a more general solvable L we will first prove:

THE LOCAL STRUCTURE THEOREM. *Suppose L is a finite-dimensional solvable Lie p-algebra over the algebraically closed field F of characteristic $p > 2$, T is a maximal torus in L, χ is a linear form on L, and $u(L) = u(L, \chi)$. Then we have the following*:

(1) *There exists a maximal radical torus $SZ(L)$ for $u(L)$ which is a p-torus and commutes with T.*

(2) *If e is a primitive radical idempotent in $SZ(L)$ and $\dim_F eu(L)e / eR(L)e = p^{2m(e)}$, then, for $1 \leq i \leq m(e)$, there exist s_i, a_i in $eu(L)e$ such that*:

(a) $Te \subset Fe + \Sigma Fs_i$.

(b) $s_i^p = s_i$, $a_i^p = e$, $[s_i, s_j] = 0 = [a_i, a_j]$, $[s_i, a_j] = \delta_{i,j} a_j$ *for all* i, j.

(c) $eu(L)e = \oplus \Sigma Fes^\alpha a^\beta + eR(L)e$, *where* $\alpha, \beta \in P^{m(e)}$.

[Thus (b) gives $\mathrm{Sp}\{s_i, a_j\colon 1 \leq i, j \leq m(e)\} = L_{2m(e)}$, as in 3.8, and the first summand on the right of (c) is $u(L_{2m(e)})$, hence is simple].

4.4. Given the maximal torus T of L we choose a sequence $L = J_s \supset \cdots \supset J_0 = \{0\}$ of p-ideals of L forming a composition series for the adjoint representation of L and such that $T_i = T \cap J_i$ is a maximal torus in J_i. Thus J_{i-1} is maximal in J_i as a p-ideal of L, and, as in [11, p. 87], we have $[J_1, J_i] \subset J_{i-1}$ and either $J_i^{[p]} \subset J_{i-1}$ or $J_i = Ft + J_{i-1}$ for some $t \in T$ with $t^{[p]} = t$. The proof of 4.3 will be by induction. For $s = 1$, J_1 is strongly solvable and we can use 4.2. To proceed further we first need several preliminary results.

4.5. LEMMA. *Suppose B is a Lie subalgebra of $u(L)$, $[L, B] \subset B$ and such that all $u \in B$ are nilpotent. Then $B \subset R(L)$.*

Proof. We will have $\nabla(u(L))(B) \subset B$. Suppose R is an irreducible representation of L on the vector space V and $V_B = \{v: R(B)v = 0\}$. Then $V_B \neq 0$ and hence $V = \sum R(x^\alpha)V_B$, where $\{x_i\}$ is a basis of L. From the formula in 2.1, since $\nabla(x^\alpha *)(u) \in B$, we obtain $R(u)R(x^\alpha)V_B = 0$ for any u in B. Hence $R(B) = 0$ and we must have B contained in the radical.

4.6. LEMMA. *Suppose K is a p-ideal of L. Then the following hold*:

(1) *Every semisimple element of $Z(K)$ lies in $Z(L)$.*

(2) *Every radical idempotent for $u(K)$ is one for $u(L)$.*

(3) *Let $Z_L(K) = \{u \in u(K): [u, K] \equiv 0\} \subset Z(K)$. Then $[Z_L(K), Z_L(K)] \equiv 0$ and $Z_L(K)^p \subset Z(L)$.*

(4) *Each homomorphism of $Z(L)$ onto F has a unique extension to a homomorphism of $Z(L)Z_L(K)$.*

Proof. For (1) we may assume $s^p = s$. If $U_i = \{u \in u(K): [s, u] = iu, 0 \leq i \leq p - 1\}$, then $u(K) = \oplus \sum U_i$. Let $B = \sum U_i + \sum [U_i, U_{-i}]$, $0 \leq i \leq p - 1$. Then $B \subset R(K)$ and $[U(K), B] \subset B$. For $x \in L$, with $x_i = (1 - (\delta(s) - i)^{p-1})x$, we have $x_i \in B$ for $i \neq 0$, $[x_0, s] = 0$, $[x_0, B] \subset B$, and $x \equiv x_0$, modulo $u(K)$. Thus $[L, B] \subset B$. Since B is nil, then 4.5 gives $B \subset R(L)$ and hence $s \in Z_L(K)$. Since $[L, s] \subset u(K)$, $s^p = s$ implies $s \in Z(L)$. Thus (1) holds and (2) follows immediately.

For (3), we have $[L, Z_L(K)] \subset Z_L(K)$ and $[Z_L(K), Z_K(K)]$ is nil so that 4.5 applies to give the congruence. Suppose $u \in Z_L(K)$. Then $[u, u(K)] \equiv 0$ implies $[u, [u, u(L)]] \equiv 0$ so $[u^p, L] \equiv 0$ and $u^p \in Z(L)$. For (4) we can extend ρ to $Z_L(K)$ by letting $\rho(u) = \rho(u^p)^{1/p}$.

4.7. For the inductive step we now take $k > 0$, $J = J_k$, $K = J_{k-1}$, and assume the structure theorem holds for K. More explicitly, we assume $SZ(K)$ has been constructed as a maximal radical p-torus for $u(K)$, commuting with T, and $e \in SZ(K)$ is a primitive radical idempotent for $u(K)$ with associated homomorphism ρ. We let $m(K, e)$ be the nonnegative integer such that the simple matrix algebra $eu(K)e/eR(K)e$ is of dimension $p^{2m(K,e)}$. We further assume that the s_i, a_j are root vectors for $\delta(T)$ acting on $u(K)$ with $[T, s_i] = 0$. For $S(K, e) = \sum Fs^\alpha a^\beta$, we have $s(K,e)$ is a simple matrix algebra of dimension $p^{2m(K,e)}$ with $\sum Fs^\alpha$ as a maximal torus, hence containing $Te \cap K$. The induction lemmas (Lemmas 4.13 and 4.14) will be used to extend the construction to J.

4.8. LEMMA. *Suppose* $d, a \in eu(K)e$, $d^p, a^p \in Fe$, *and* $[d, a] = e$. *For* $u \in eu(L)e$, *let* $P_a(u) = \Sigma((-1)^k/k!)\delta(a)^k(u)d^k$ *and* $Q_d(u) = \Sigma(1/k!)\delta(d)^k(u)a^k$, $0 \le k \le p-1$. *Then*:

(1) P_a *is idempotent and projects* $eu(L)e$ *on* $C(a) = \{u: [a, u] = 0\}$.

(2) Q_d *is idempotent and projects* $eu(L)e$ *on* $C(d) = \{u: [d, u] = 0\}$.

(3) P_a *and* Q_d *commute and* $Q_d C(a) \subset C(a)$.

(4) $eu(L)e = \oplus \Sigma C(a)d^i = \oplus \Sigma C(d)a^j = \oplus \Sigma C(a, d)\, d^i a^j$, *where* $C(a, d) = C(a) \cap C(d)$.

(5) *For* $x \in L$, $exe \equiv P_a(exe) \equiv Q_d(exe) = Q_d P_a(exe)$, *modulo* $eu(K)e$.

(6) *If* d, a *are root vectors for* $\delta(T)$ *associated with the roots* κ, λ *then* $\kappa + \lambda = 0$ *and* P_a, Q_d *leave the root spaces of* $\delta(T)$ *invariant. For* $t \in T$, $Q_d P_a(t) = t - \lambda(r)ad$.

Proof. Since $[e, u] = 0$ we have $[a, P_a(u)] = 0$ so $P_a(u) \in C(a) \subset \{u: P_a(u) = u\}$. Thus (1) follows and (2) holds similarly. (3) is a consequence of $[\delta(a), \delta(d)] = \delta(e) = 0$. The same proof as used in [10, Proof of Lemma 4.3, p. 228] now can be used to give (4) with the third equality using invariance of $C(a)$ under Q_d. All parts of (5) follow from the invariance of $eu(K)e$ under $\delta(exe)$ and the Poincaré–Birkhoff–Witt theorem.

For (6), $[T, e] = 0$ implies $\kappa + \lambda = 0$. Hence, if u is a root vector for the root σ, $\delta(d)^i(u)a^i$ will lie in the same root space as u, so Q_d leaves root spaces invariant and a similar result holds for P_a. Now $P_a(t) = t + [a, t]d = t - \lambda(t)ad$. It follows readily that $Q_d P_a(t) = t + \lambda(t)ad$.

4.9. LEMMA. *Let* $d_i = a_i^{p-1}s_i \in u(K, e)$. *Then* d_i *is a root vector for* T, $[d_i, a_j] = \delta_{i,j}e$, $[d_i, d_j] = 0$, *and* $d_i^p = 0$.

Proof. Since a_i is a root vector for T, a_i^k will also be one and thus the same will hold for d_i. We have $[d_i, a_i] = a_i^p = e$ and $[d_i, a_j] = 0$. Also $[s_i, a_j^{p-1}] = -\delta_{i,j}a_j^{p-1}$, which leads to $[d_i, d_j] = 0$. Induction on k and $a^{-1} = a^{p-1}$ gives $d_i^k = (a_i^{-k})(s_i)\cdots(s_i - (k-1))$ so that $d_i^p = a^p(s_i^p - s_i) = 0$.

4.10. LEMMA. *Let* $P_i = P_{a_i}$ *and* $Q_i = Q_{d_i}$. *Then*:

(1) $\{P_i, Q_j\}$ *is commutative*.

(2) *If* $P = \prod P_i$, $Q = \prod Q_i$, *then* P, Q *and* PQ *are idempotent and commute*.

(3) *Suppose* $S(K, e) \subset U \subset eu(L)e$ *and* U *is invariant for all* P_i, Q_j. *If* $C(a_i) = P_i(U)$, *then* $U = \oplus \Sigma C(a_i)d_i^k$, $0 \le k \le p-1$, *and if* $C(a_i, d_j) = Q_j C(a_i)$, *then* $U = \oplus \Sigma C(a_i, d_j)\, d_i^k a_j^1$, $0 \le k, 1 \le p-1$.

(4) $QP(U) = \{u: [S(K, e), u] = 0\}$.

(5) *If* $U_0 = QP(U)$, *then* $U = \oplus \sum U_0 d^{\alpha} a^{\beta}$.

(6) *Let* $C = C(K, e) = QP(eu(K)e)$ *and* $C' = C'(K, e) = C \cap eN(K)e$. *Then* $C = Fe + C'$ *and* $eN(K)e = \oplus \sum C' d^{\alpha} a^{\beta}$.

Proof. (1)–(5) follow readily by repeated use of 4.9. For (6) the simplicity of $S(K, e)$ gives $C \cap S(K, e) = Fe$ and the decomposition for C is obtained since $eu(K)e = S(K, e) + eN(L)e$, while the last sum comes from (3) applied to $eu(K)e$.

4.11. LEMMA. (1) *for* $x \in L$ *there exist* $u(x) \in eu(K)e$ *and* $z(x) \in eu(L)e$ *such that* $exe = u(x) + z(x)$ *and* $[z(x), S(k, e)] = 0$.

(2) $[z(x), C] \subset C$, $[L, C] \subset C + N_L(K) \subset Z_L(K)$, $C \subset Z_L(K)$, *and* $[C, C] \equiv 0$.

(3) $[x, z(y)] \equiv [z(x), z(y)] \equiv z([x, y])$ *and* $[u(x), u(y)] \equiv u([x, y])$.

(4) *If* a_i *is associated with the root* λ_i *for* T, *then for* $t \in T$, $z(t) = et - \sum \lambda_i(t) a_i d_i$ *and* $[T, u(t)] = 0$.

Proof. If $m(K, e) = 0$, then $S(K, e) = Fe$ and we can set $z(x) = exe$ and $u(x) = 0$. Thus we may assume $m(K, e) > 0$ and let $z(x) = QP(exe)$ and $u(x) = exe - z(x)$. Then $z(x)$ commutes with all d_i, a_j and hence with all s_i as well so $[z(x), S(\rho, K)] = 0$. We have $u(x) \in eu(K)e$ since $[x, u(K)] \subset (K)$ and the definitions of P_i and Q_j show that $exe \equiv z(x)$, modulo $eu(K)e$.

Now $[z(x), S(\rho, K)] = 0$ implies $[z(x), C] \subset C$. Now $x = exe + ex(1 - e) + (1 - e)x)e + (1 - e)x(1 - e)$ and the two middle terms lie in $R(L)$. Thus $[x, C] \subset C + R(L)$. Since $C \subset u(K)$, $[L, C] \subset C + Z_L(K) \subset Z_L(K)$. Now $C + R(L)$ is invariant for $\delta(L)$ and $[C + R(L), u(K)]$ is nil. Thus, by 4.5, $[C, u(K)] \equiv 0$ so $C \subset Z_L(K)$ and hence $[C, C] \equiv 0$.

The decomposition of x relative to e used above gives the first congruence for (3) and also shows $x \equiv u(x) + z(x)$ for all x. Thus, $u([x, y]) + z([x, y]) \equiv [x, y] \equiv [u(x) + z(x), u(y) + z(y)] \equiv [u(x), u(y)] + [z(x), z(y)]$. From this we can obtain the other two congruences.

4.12. LEMMA. *Let* $A = A(K, e) = \oplus \sum Ca^{\beta}$ *and* $A' = A'(K, e) = \oplus \sum C'a^{\beta}$. *Then* $A + Z_L(K)$ *is strongly solvable, invariant under* $\delta(L)$, $A' \subset eZ_L(K)e$, *and* A, A' *are invariant for* $\delta(eLe)$. *For* $x \in L$, $z \in C$ *we have* $\rho([x, z]) = \rho([exe, z]) = \rho([z(x), z])$.

Proof. C is a subalgebra containing Fe and it follows readily that A is a subalgebra with $[A, A] \subset A' \subset eR(K)e$. Also A, A' are invariant for $\delta(S(e))$ and $\delta(C)$ so that A, A' are Lie ideals for $eu(K)e$ with A strongly solvable and A' nil.

Suppose $x \in L$ and $exe = z(x) + u(x)$ as in 4.11. Then, from the decomposition for x relative to e, $\rho([x, z]) = \rho([exe, z]) = \rho([u(x) + z(x), z]) = \rho([z(x), z])$.

4.13. *Proof of the induction lemma for $J^{[p]} \subset K$.* There are two cases to consider:

Case 1. Suppose $\rho([J, C]) \neq 0$. If $C(0) = \{u \in C\colon [J, u] \equiv 0\}$, then $C(0)$ is properly contained in C and $C(0) = Z_L(J) \cap C$. Thus we can choose $C(1)$ such that $C(0) \subset C(1) \subset C$ and $\delta(L)$ acts irreducibly on $C(1)/C(0)$. We have $C(0)C(1) \subset eC(1) + C'(0) \subset C(1)$. Since $\delta(L) = \delta(eLe)$ on $C(1)/C(0)$, $\delta(eJe)$ acts as nilpotent operators on $C(1)/C(0)$ and we have $[eJe, C(1)] \subset C(0)$. If $\rho([eJe, C(1)]) = 0$, then $[J, C(1)]$ is both nil and $\delta(L)$-invariant so that $[J, C(1)] \equiv 0$ and $C(1) \subset C(0)$, a contradiction.

From 4.12 we have $\rho([z(eJe), C(1)] \neq 0$ and can choose $x_1 \in J$, with x_1 a root vector for T and a root vector $b_1 \in C(1)$ such that $[z(x_1), b_1] = w = e + z$, where z is nilpotent and in $C'(0)$. Then w is invertible with order p^k, where k is the least integer with $z^{p^k} = 0$. Thus, if b_1 is replaced by $w^{-1}b_1$, then $[z(x_1), b_1] \equiv e$ and $[z(eJe), b_1] \subset C(0)$. Let $b_2', \ldots, b_r'$ be a basis for $C(1)$ supplementary to $Fb_1 + C(0)$ and let $b_i = b_i' - [z(x_1), b_i']b_1$. Then $[z(x_1), b_i] \equiv 0$ for $i > 1$ and thus $[z(x_1), C(1)] \subset Fe + R(L)$. Since $\{x \in J\colon [z(x), C(1)] \subset Fe + R(L)\}$ is an ideal of L containing $Fx_1 + K$, we thus have $[J, C(1)] \subset Fe + R(L)$ and can define a bilinear form on $J \times C(1)$ by setting $(x, b) = \rho([z(x), b])$. For $y \in L$ we will have $([x, y], b) = (x, [y, b])$ and from this we can conclude that J/K and $C(1)/C(0)$ are paired. Thus, if $x_1, \ldots, x_r$ is a basis for J supplementary to K with each a root vector, there will exist root vectors $b_1, \ldots, b_r$ in $C(1)$ such that $[z(x_i), b_j] \equiv \delta_{i,j}e$. Since $[x_i, T \cap K] = 0$ and $z(x) \equiv x$, mod $u(K)$, we have $[z(x_i), T \cap K] = 0$ and $[b_i, T \cap K] = 0$. Then $ex_ie \equiv z_i$ mod $u(K)$, $z_i^p \equiv 0$, and $[z_i, b_j] \equiv \delta_{i,j}e$. Now $[z_i, C] \subset C$ and C is a subalgebra of $u(K)$ so that if $B = \sum z^\alpha C$, then B is an associative subalgebra. We have $[C, C] \equiv 0$, $[z_i, z_j] \in C$, and all $b_i \in C$. If R is an irreducible representation of B on V, then there will exist some nonzero $v_0 \in V$ with $R(a)v_0 = \rho(a)v_0$ for $a \in C$. Then V is spanned by $\{R(z^\alpha)v_0\}$ and $[z_i, b_j] = \delta_{i,j}e$ implies this spanning set is independent so $\dim(V) = p^{J/K}$. From this we obtain $B = \sum Fz^\alpha b^\beta + \mathrm{Rad}(B)$ and $B/\mathrm{Rad}(B)$ is simple of dimension $p^{2\dim(J/K)}$. Also $\sum Fez^\alpha b^\beta S(\rho, K) + \mathrm{Rad}(B)$ will be simple with dimension $p^{2(\dim(J/K)+m(K,e))}$. Thus $eu(J)e/eN(J)e$ will be a simple algebra of dimension $p^{2(m(K,e)+\dim(J/K))}$. Most of the remainder of the proof is to show that the congruences for the z_i, b_j can be replaced by equations.

We let $z = z_k$, $b = b_k$, and $t = bz$. Then $[t, b] \equiv b$ and $[t, z] \equiv -z$. Thus $bt \equiv (t - e)b$ and $zt \equiv (t + e)z$, and an induction on k gives $b^k z^k \equiv t(t + e)\cdots(t + (k - 1))$. With $k = p$ this gives $t^p - t \equiv \prod(t + ke) \equiv z^p b^p$.

Now $z^p \in C$ and thus, for k sufficiently large, $t^{p^{k+1}} - t^{p^k} = \eta e$ for some scalar η. Thus there is some λ such that if t is replaced by $t^{p^k} - \lambda e$, we will have $t^p = t$. Now $[z, b] = e$ implies the roots corresponding to z, b are additive inverses so that $[T, t] = 0$. Also $[t, b] \equiv b$. If b is now replaced by $(1 - (\delta(t) - 1)^{p-1})(b)$, we may assume $[t, b] = b$. Then $\{et^i b^j\colon 0 \leq i, j \leq p - 1\}$ will be linearly independent. If B_k is the subalgebra of B generated by t, b, e, then $B_k/\mathrm{Rad}(B_k)$ will be simple and of dimension p^2. Since $b^p \in Z(L)$, $\mathrm{Rad}(B_k) \subset R(L)$.

If b is nilpotent, then $b + \mathrm{Rad}(B)$ will generate a nil ideal in $B/\mathrm{Rad}(B)$ which implies $b \equiv 0$. Thus we may assume b is a unit and $b^p = e + r$, where $r \in \mathrm{Rad}(B) \cap R(L)$. If $g = b^{-1}t$, then $[g, b] = e$, $[t, g] = -g$, and $g^p = 0$. Let $u = -(b + t)$ and $v = g + e$. Then $[u, v] = v$ and $v^p = e$ so that if s is the semisimple component of u, $[s, v] = v$ and hence there is some $s \in B$ with $s^p = s$ and $[s, v] = v$. Then the subalgebra A generated by s and v will be simple and of dimension p^2 so that $B_k = A \oplus \mathrm{Rad}(B_k)$. Thus there exist $s_1, b_1 \in A$ and $z_1, z_2 \in \mathrm{Rad}(B)$ with $t = s_1 + z_1$ and $b = b_1 + z_2$. This then implies $s_1^p = s_1$, $b_1^p = e$, and $[s_1, b_1] = b_1$. Now $[T, u], [T, v] \subset A$ imply $[T, A] \subset A$ and also $[T, \mathrm{Rad}(B_k)] \subset \mathrm{Rad}(B_k)$. This implies $[T, s_1] = 0$ and b_1 is a root vector. Thus we may replace t by s_1 and b by b_1.

We now set up an induction procedure to complete the proof for Case 1. If $g_1 = b_1^{p-1}t_1$, then $[g_1, b_1] = e$, $g_1^p = 0$, and $b_1^p = e$. We define P_1, Q_1 as in 3.4 using g_1, b_1 in place of d, a. Then $eu(J)e$ and $z(eu(J)e)$ are invariant under P_1, Q_1 and $z(x) \equiv Q_1P_1(z(x))$ modulo $eu(K_1)e$, where $K_1 = Fx + K$. Also $\rho([z(x), u]) = \rho([Q_1P_1(z(x)), u]) \in C_1 = Q_1P_1(eu(K_1)e)$. Thus the argument given above applied to z_2, b_2 will give t_2, b_2 as root vectors for T satisfying the desired equations and commuting with $\{t_1, b_1\}$ as well as $S(K, e)$. We can continue in this way until J is attained. We now let $S(J, E)$ be the subalgebra generated by $\{s_i\} \cup \{t_j\} \cup \{a_i\} \cup \{b_j\}$. Then $S(J, e)$ is a simple associative algebra. If we use the new t_i, b_j to construct projections P, Q we can let $C(J, e) = QPC(K, e)$ and obtain $eu(J)e = \oplus \Sigma C(J, e)S(J, E)$, completing the proof.

Case 2. $\rho([J, C]) = 0$. Thus $[J, C] + R(L)$ is nil and $\delta(L)$-invariant; hence, $[J, C] \equiv 0$. Thus $C \subset Z_L(J) \cap u(K)$, $C' \subset R(J)$, and, for $x \in J$, we have $[z(x), eu(K)e] \equiv 0$. This implies $z([J, J])$ and $z(x)^p$ lie in $C \cap Z_L(J)$ so $[x, z(y)] \equiv [z(x), z(y)] = \rho([x, z(y)])e + z(x, y)$, where $z(x, y) \in R(J)$.

Now we let $B = eJeC + C + R(L) = z(J)C + C + R(L)$. Then B is $\delta(L)$-invariant and $[B, B] \subset [z(J), z(J)] + R(L)$.

Suppose, $x_1, y_1 \in J$ and $\rho([x_1, z(y_1)]) = 1$. Then $[z(x_1), z(y_1)] = w$, where w is a unit in $Z_L(J)$. Hence $[z(x_1), z(w^{-1}y)] = [z(x_1), w^{-1}z(y_1)] \equiv w^{-1}[z(x_1), z(y_1)] = e$. Let $b_1 = w^{-1}y_1$. If $w = e + z$, where $z \in N(J)$, then $e - w$ is nilpotent and $w^{-1} = \Sigma(e - w)^k$, so $b_1 \equiv y_1$, modulo $eu(K)e$.

Also $b_1 \in CJ$ and $[z(x_1), b_1] = e$. If $b_2', \ldots, b_r'$ is chosen as a basis for CJ supplementary to Fb_1 and $b_i = b_i' - [z(x_1), b_i']b_1$, then $[z(x_1), b_i] \equiv 0$ for $i > 1$ and hence $[z(x_1), CJ] \subset Fe + R(L)$ so $[z(x_1), B] \subset Fe + R(L)$. If $J' = \{x \in J: [z(x), B] \subset Fe + R(L)\}$, then J' is an ideal of L containing K and x_1; hence, $J' = J$. Thus $[z(J), z(K)] \subset Fe + R(L)$ so $(x, y) = \rho([z(x), z(y)])$ defines a skew-symmetric bilinear form on $J \times J$ with $(K, J) = 0$ and $([J, L], J) = (J, [L, J])$. Since $(x_1, y_1) = 1$ this implies $(J, J) \neq 0$ and $K = \{x: (x, J) = 0\}$. Thus the form is nondegenerate on J/K and $\dim(J/K)$ must be even. Since L acts irreducibly on J/K this dimension must be a power of p, giving a contradiction.

We now have $[J, z(J)] \equiv [z(J), z(J)] \equiv 0$. Since $eu(J)e = z(J) + eu(K)e$ we have $eu(J)e \subset Z_L(J)eu(K)e \subset S(\rho, K) + eR(J)e$. Thus, with $SZ(J) = SZ(K)$, the induction hypothesis now applies to J.

4.14. *Proof of the induction lemma for* $J = Ft + K$. We have $te = ete = u(t) + z(t)$, where $u(t) = -\sum \lambda_i a_i d_i = -\sum \lambda_i s_i$. If $s = t - \lambda 1$, where λ is chosen such that $s^p = s$, then $u(s) = u(t)$ and $z(s) = z(t) - \lambda e$. Thus $u(s)^p = u(s)$ and $z(s)^p = z(s)$. Again we distinguish two cases.

Case 1. $\rho([t, C]) \neq 0$. Thus there exist $w \in C$ such that w is a root vector for T, $[t, w] \neq 0$, and $\rho(w) = 1$. Then w is a unit and we may assume $[s, w] = w$. Thus $[z(s), w] = w$. We can now use the same argument as in 4.13 to obtain s_0, a_0 with $[T, s_0] = 0$, a_0 a root vector for T, and such that the augmented sets $\{s_i\}, \{a_i\}$, $i = 0, \ldots, m(K, e)$, will generate a simple algebra $S(J, e)$ of dimension $p^{2(m(K,e)+1)}$.

Case 2. $\rho([t, C]) = 0$. Then $\rho([s, C]) = 0$ and $[J, C] \subset C'$ so $[J, C] \equiv 0$ and $[z(s), u(K)] \equiv 0$. Now $\lambda_i \in P$ so $u(s)^p = u(s)$ and $z(s)^p = z(s)$. Since $[s, u(s)] = 0$ we have $[u(J), z(s)]$ is nil and $z(s) \in Z(L)$. This gives $z(s) = \sum i f_i$, where f_i is a radical idempotent and $e = \sum f_i$. Then, for $e_i = ef_i$, e_i is a radical idempotent for each i and $e = \sum e_i$. Since $e \in u(K)$ and $f_i \notin u(K)$, $e_i \neq 0$. We now set $S(e_k) = \sum F(e_k s_i)^\alpha (e_k a_j)^\beta$. Then $S(e_k)$ is isomorphic to $S(K, e)$ and hence is a simple matrix algebra, so e_k is a primitive idempotent in $u(J)$. We have $eu(K)e = \oplus \sum_k (S(e_k + e_k N(J) e_k)$ and the desired relations hold for each $e_k u(J) e_k$.

We now let $SZ(J) = SZ(K) + \sum Fe_\rho z_\rho^i$, where the latter sum is taken over all ρ for which Case 2 occurs.

4.15. *The Proof of the structure theorem*. The theorem holds for J_1, and 4.13 and 4.14 allow the induction to continue until $J = L$. We note that the construction given is compatible with the sequence $\{J_i\}$, i.e., $S(J_i, e) = S(L, e) \cap e_i u(J_i) e_i$, where e_i is obtained by restricting ρ to $Z_L(J_i)$.

4.16. COROLLARY. *With the notation of the structure theorem let* $T(e) = \sum Fes^{\alpha}$, $S(e) = \sum T(e)a^{\beta}$, $C(S(e)) = \{u \in eu(L)e\colon [S(e), u] = 0\}$, *and* $C'(S(e)) = C(S(e)) \cap eR(L)e$. *Then*:

(1) $S(e)$ *is a simple matrix algebra with* $T(e)$ *as a maximal torus which commutes with* T.

(2) $eu(L)e = \oplus \sum C(S(e))s^{\alpha}a^{\beta}$, $C(S(e)) = Fe + C'(S(e))$, *and* $eR(L)e = \oplus \sum C'(S(e))s^{\alpha}a^{\beta}$.

(3) $T(e)$ *is a maximal torus for* $eu(L)e$ *with root spaces* $C(T(e))a^{\beta}$, *where* $C(T(e)) = \{u\colon [T(e), u] = 0\} = C(e)T(e)$.

(4) *For* $\eta \in P^{m(L)}$ *the idempotents* $e_{\eta} = \prod_i (1 - (s_i - \eta_i)^{p-1})$ *will be primitive in* $u(L)$ *and give a basis of orthogonal idempotents for* $T(e)$.

Proof. Apart from the assertions regarding $T(e)$, (1) and (2) follow from 4.8 and 4.12, using the structure theorem for L rather than K. For any β, we have $[s_i, a^{\beta}] = \beta_i a^{\beta}$, so $\{a^{\beta}\}$ will consist of root vectors for $T(e)$ corresponding to distinct roots and $S(e)$ is then a direct sum of one-dimensional root spaces for $T(e)$. This implies $T(e)$ is a maximal torus for $S(e)$, giving (1) and (2).

For β fixed, $C(e)T(e)a^{\beta}$ will consist of root vectors for the same root as a^{β}, and (2) shows that $eu(L)e$ is a direct sum of these. Thus $T(e)$ will be a maximal torus for $eu(L)e$ and (3) holds, while (4) follows from the results of Section 3.

4.17. THE GLOBAL STRUCTURE THEOREM. *With the notation of* 4.16 *let* $SZ(L) = \sum Fe_{\rho}$, $S(L) = \sum S(e_{\rho})$, *and* $T(u(L)) = \sum T(e_{\rho})$. *Then* $S(L)$ *is a semisimple algebra,* $u(L) = S(L) \oplus R(L)$, $T(u(L))$ *is a maximal torus for* $u(L)$ *containing* T, *and* $SZ(L)$ *is a maximal radical torus for* $u(L)$.

Proof. We have $u(L) = \sum e_{\rho}u(L)e_{\rho} + R(L)$. Since $T(\rho)$ is a maximal torus for $e_{\rho}u(L)e_{\rho}$, $T(u(L))$ will be maximal in $u(L)$. Then $[T, T(u(L))] = 0$ implies $T \subset T(u(L))$. It follows from the construction that $SZ(L)$ is a maximal radical torus.

5. APPLICATIONS

5.1. With notation as in Section 4 we now set $A(e_{\rho}) = \sum C(S(e_{\rho}))a^{\beta}$ and $A'(e_{\rho}) = \sum C'(S(e_{\rho}))a^{\beta}$ as in 4.12 and let $A = \sum_{\rho} A(e_{\rho})$, $A' = \sum_{\rho} A'(e_{\rho})$. Thus A is strongly solvable, $SZ(L)$ is a maximal torus in A, and $[L, A] \subset A + R(L)$. For $a \in A$ we will have $a^p \in Z(L)$ and thus each homomorphism ρ of $Z(L)$ has a unique extension, also denoted by ρ, to a homomorphism of $A + R(L)$ with $\rho(A(e_{\sigma})) = 0$ for $\sigma \neq \rho$. For $a \in SZ(L)$ we have $ae_{\rho} = \rho(a)e_{\rho}$. As noted in Section 3, for each irreducible χ-repre-

sentation R of L there will exist a unique e_ρ with $R(e_\rho) = 1$. For this ρ and $a \in A + R(L)$ we have $R(a) = \rho(a)1$. 5.2 shows that A is sufficiently large to determine, up to equivalence, all irreducible χ-representations of L.

5.2. THE STRUCTURE THEOREM FOR IRREDUCIBLE REPRESENTATIONS. *Suppose R is an irreducible χ-representation of L on V, $e_\rho \in SZ(L)$ with $R(e_\rho) = 1$, and ρ is the associated homomorphism of A. Let $V_\rho = \{v: R(a)v = \rho(a)v$ for all $a \in A\}$ and $d_i = a_i^{p-1}s_i$, $1 \le i \le m(e_\rho)$. Then the following hold*:

(1) *V_ρ is one dimensional and is the unique minimal subspace for A.*

(2) *If $V_\rho = Fv_0$, then $\{R(d^\alpha)v_0\}$ is a basis for V.*

(3) *$R(A)$ is a maximal commutative subalgebra in $\mathrm{Hom}_F(V, V)$ and $[R(L), R(A)] \subset R(A)$.*

Proof. $R(A)$ is commutative and hence has a one-dimensional invariant subspace Fv_0. Since $R(a) = \rho(a)1$ for a in $Z(L)$, we have $v_0 \in V_\rho$. From the structure theorem we obtain V is spanned by $\{R(d^\alpha)v_0\}$. We have $R(a_i)R(d^\alpha)v_0 = -\alpha_i R(d^{\alpha-\varepsilon_i})v_0$ where ε_i is the vector consisting of 0s except for 1 in position i. It is then easy to prove linear independence and that Fv_0 is the unique minimal subspace for A, hence equal to V_ρ.

Suppose $u \in eu(L)e$ and $[R(u), R(A)] = 0$. Then $R(u) = \sum c_{\alpha,\beta}R(d^\alpha a^\beta)$, where $c_{\alpha,\beta} \in F$. Since $R(a^\beta)v_0 = \rho(a^\beta)v_0$ and $R(u)V_\rho \subset V_\rho$ we must have $c_{\alpha,\beta} = 0$ for $\alpha \neq 0$ and $R(u) \in R(A)$. Since $R(u(L)) = \mathrm{Hom}_F(V, V)$, $R(A)$ is maximal as a commutative subalgebra. Since $[L, A] \subset A + R(L)$ the last inclusion follows.

5.3. To relate 5.2 to the results obtained in [8] and [12], for a fixed homomorphism ρ of A we define a bilinear form in $L \times A$ by $(x, a) = \rho([x, a])$ and let $L_\rho = \{x: (x, A) = 0\}$. Then L_ρ is a p-subalgebra and equal to $\{x: [x, Ae_\rho] \subset A'e_\rho + R(L)\}$. If $\dim(L/L_\rho) = r$ and $\{x_i\}$ is a basis for L supplementary to L_ρ, then there exist $b_i \in A$ with $(x_i, b_j) = \delta_{i,j}$ and $\rho(b_j) = 0$. If R is an irreducible χ-representation on V with $R(e_\rho) = 1$ and $V_\rho = \{v: R(a)v = \rho(a)v\}$ then $L_\rho = \{x \in L: R(x)V_\rho \subset V_\rho\}$. By the same proof as used for Theorem 1 in [7] we obtain $\dim(V) = p^r\dim(V_\rho)$. From 5.2 we have $\dim(V_\rho) = 1$ and hence R is the representation induced by the one-dimensional representation of L_ρ acting on V_ρ. This also gives $m(e_\rho) = \dim(L/L_\rho)$.

In general L_ρ is not an ideal of L. However, if $J = L \cap A$, then $J \subset L_\rho$ for all ρ and J is an ideal of L. It follows then that J is strongly solvable and, as such, is maximal in L. Conversely, given any maximal strongly solvable ideal J of L, J can be taken as an ideal in the sequence $\{J_i\}$ used to construct A; thus, $J = A \cap L$ for some A.

5.4. Two (related) questions of general interest for $u(L)$ involve the structure of the center and the blocks. To this end we let $SZ_0(L) = \{s \in SZ(L)\colon [s, L] = 0\}$ so that $SZ_0(L)$ is a maximal torus for the center for $u(L)$. For homomorphisms ρ, σ we will say $\rho \sim \sigma$ if $\rho = \sigma$ on $SZ_0(L)$. This defines an equivalence relation on $\{\rho\}$ and is useful in describing the block decomposition for $u(L)$. Suppose ρ, σ are inequivalent. Then there is some $s \in SZ_0(L)$ with $\rho(s) \neq \sigma(s)$. For $u \in e_\rho u(L) e_\sigma$, we have $0 = [s, u] = \rho(s) - \sigma(s)u$ and thus $e_\rho u(L) e_\sigma = 0$. Now the global structure theorem gives a complete set of primitive idempotents, and each of these will be a direct summand of some unique e_ρ. Then, by making use of [1, Sect. 55, Exercise 3], it follows that if $e_{[\rho]} = \sum e_\sigma$, with the sum taken over all $\sigma \in [\rho]$, then $e_{[\rho]}$ is central primitive and the blocks for $u(L)$ are given by $e_{[\rho]} u(L) = \sum e_\rho u(L) e_\sigma$, $\sigma \in [\rho]$. If L is strongly solvable, then 4.2 gives $e_{[\rho]} = f_\rho$.

For the general case the induction lemma shows that a primitive radical idempotent e in $u(K)$ remains primitive in $u(J)$ unless $J = Ft + K$ and $t \in T_\rho = L_\rho \cap T$. In this case e decomposes $e = \sum e_i$, $0 \leq i \leq p - 1$, where the e_i are orthogonal primitive radical idempotents in $u(J)$. Thus $SZ(L)$ will have a basis consisting of $\sum_\rho p^{\dim(T_\rho)}$ orthogonal primitive radical idempotents and $u(L)/R(L)$ will have this number of simple components.

The proof of the structure theorem also can lead to a construction of the central idempotents in $u(L)$. In the induction process used in 4.13 and 4.14, to pass from $u(K)$ to $u(J)$, suppose f is a primitive central idempotent in $u(K)$ and $f = \sum e_\rho$, where each e_ρ is a primitive radical idempotent in $SZ(K)$. Then f will be central and remain primitive in $u(J)$ except, perhaps, if $J = Ft + K$ and Case 2 holds. We have $tf = \sum te_\rho = z(t) + u(t)$, where $z(t) = \sum z_\rho(t)$, $u(t) = \sum u_\rho(t)$, $u(t) \in \sum T(\rho, K)$, and $[z(t), u(K)f] \equiv 0$. For congruence to be replaced by equality it is necessary and sufficient that $\delta(tf) = \delta(u(t))$, i.e., $\delta(tf)$ is an inner derivation of $u(K)f$. If this occurs, then $z(t)$ is central in $u(L)$ and will provide primitive central idempotents in $u(J)$ by using the $e_j f$, where $z(t) = \sum j e_j$. An example of this situation is given in the diamond algebra of [2, Example 1].

From consideration of examples like the diamond algebra it appears that a result like that in 4.2(6), for L strongly solvable, should hold generally for L solvable, but we do not yet have a proof.

In order to obtain further results on the block structure of $u(L)$ it will be necessary to consider the components $e_\rho u(L) e_\sigma$ with $\rho \sim \sigma$, $\rho \neq \sigma$, and the action by left (right) multiplication on them by $e_\rho u(L) e_\rho$ $[e_\sigma u(L) e_\sigma]$. For this purpose we define $Dg(L)$ as the diagonal subalgebra $Dg(L) = \sum e_\rho u(L) e_\rho$, and let $C(L) = \sum C(\rho)$ and $C'(L) = \sum C'(\rho)$. We conclude by listing some basic properties of $Dg(L), C(L)$, and $C'(L)$.

5.5 PROPOSITION. (1) *$C(L)$ is strongly solvable with $[L, C(L)] \subset R(L)$ and $C'(L) = C(L) \cap R(L)$.*

(2) *$SZ(L)$ is a maximal torus for $C(L)$ and $C(L) = SZ(L) + C'(L)$.*

(3) *$C(L) = \{u: [S(L), u] = 0\}$ and $C(L)$ is a nilpotent Lie algebra.*

(4) *The center of $u(L)$ lies in $C(L)$.*

(5) *$Dg(L) = S(L) \oplus C'S(L)$ and $\mathrm{Rad}(Dg(L)) = C'S(L)$.*

(6) *Suppose D is a derivation of $Dg(L)$ and $D(C(L)) = 0$.*

Then there exists $u \in Dg(L)$ with $D = \delta(u)$.

Proof. For (1) we have $[L, C(L)] = \Sigma[e_\rho L e_\sigma, C(\tau)] = \Sigma[e_\rho L e_\rho, C(\rho)] \subset C'(L)$, while (2) follows directly from the definitions.

From the definitions we have $[S(L), C(L)] = 0$ and the construction of $C(L)$ gives the equation in (3); thus $[SZ(L), C(L)] = 0$ and then (2) implies $C(L)$ is nilpotent. Then (4) is an immediate consequence of (3), and (5) follows from 4.16.

For (6) we have $D(e_\rho) = 0$ for all ρ and this implies D leaves $e_\rho u(L) e_\rho$ invariant. We let D_ρ denote the restriction. With $\{d_i, a_j\}$ as in the local structure theorem we can, by using suitable modifications of the projections P, Q used in the proof, obtain $u_\rho \in S(\rho)$ such that the derivation $D_\rho - \delta(u_\rho)$ vanishes on $S(\rho)$. Since the same is true on $C(L)$, we have $D_\rho = \delta(u_\rho)$ and hence $D = \delta(\Sigma u_\rho)$ on $Dg(L)$.

ACKNOWLEDGMENT

The author would like to express his appreciation to the referee for numerous constructive criticisms and helpful suggestions.

REFERENCES

1. C. W. Curtis and I. Reiner, "Representation Theory of Finite Groups and Associative Algebras," Wiley, New York, 1988.
2. J. Feldvoss, On the block structure of supersolvable restricted Lie algebras, *J. Algebra* **183** (1996), 396–419.
3. R. Farnsteiner, Representations of Lie algebras with triangular decomposition, *in* "Symposia Gaussiana, Conference A," (Behara, Fritsch, and Lintz, Eds.), pp. 275–186, de Gruyter, Berlin, 1995.
4. B. Farnsteiner, Representations of blocks associated to induced modules of restricted Lie algebras, *Math. Nachr.* **179** (1996), 57–88.
5. N. Jacobson, "Lie Algebras," Interscience, New York, 1962.

6. J. Schue, Cartan subalgebras for Lie algebras of prime characteristic, *J. Algebra* **11** (1969), 25–52.
7. J. Schue, Representations of solvable Lie *p*-algebras, *J. Algebra* **38** (1976), 253–267.
8. J. Schue, Representations of Lie *p*-Algebras, *in* "Lie Algebras and Related Topics," (D. Winter, Eds.), pp. 191–202, Springer-Verlag, New York, 1982.
9. J. Schue, Structure theorems for the restricted enveloping algebra of a solvable Lie *p*-algebra, *Algebras, Groups and Geometries* **3** (1986), 128–147.
10. J. Schue, Enveloping algebras and division rings for Lie *p*-algebras, *Contemp. Math.* **110** (1990), 223–230.
11. J. Schue, Structure theorems for the division ring associated with a solvable Lie *p*-algebra, *Algebras, Groups, and Geometries*, **9** (1992), 81–98.
12. H. Strade, Darstellungen auflösbarer Lie-*p*-Algebren, *Math. Ann.* **232** (1978), 15–32.
13. H. Strade and R. Farnsteiner, "Modular Lie Algebras and Their Representations," Dekker, New York, 1988.